I CLAIM

1. A method for forwarding peer-to-peer content in a wireless network having a network infrastructure, **characterized in that** a wireless sender encrypts protected content or content encryption key and a wireless recipient consumes the protected content without requiring content personalization assistance from the network infrastructure.

2. A method according to claim 1, **characterized in that** the wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to the wireless recipient.

3. A method according to claim 2, **characterized in that** the wireless recipient sends a device certificate having a public key to the wireless sender.

4. A method according to claim 3, **characterized in that** the wireless sender personalizes the protected content or content encryption key for the wireless recipient.

5. A method according to claim 4, **characterized in that** the steps for personalizing include:

encrypting the content or content encryption key using a public key of the wireless recipient;

signing encrypted content or content encryption key using a private key of the wireless sender; and

sending the protected content or content encryption key together with a device certificate of the wireless sender to the wireless recipient.

6. A method according to claim 4, **characterized in that** the wireless recipient verifies forwarded protected content received from the wireless sender by:

verifying the device certificate of the wireless sender; and

applying a private key of the wireless recipient in order for the recipient to consume the protected content.

7. A method according to claim 1, **characterized in that** the protected content is digital rights management protected content.

8. A wireless network having wireless terminals and a network infrastructure for forwarding peer-to-peer content from one wireless terminal to another wireless terminal, **characterized in that** at least two wireless terminals comprise a peer-to-peer forwarding/reception of DRM protected content module for either encrypting or consuming protected content without content personalization assistance from the network infrastructure.

9. A wireless network according to claim 8, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content protocol module of a wireless sender sends an initial message having either an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

10. A wireless network according to claim 8, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender sends a device certificate having a public key to the wireless sender.

11. A wireless network according to claim 8, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender personalizes the protected content or content encryption key for a wireless recipient.

12. A wireless network according to claim 12, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender personalizes the content or content encryption key for a wireless recipient by:

encrypting the content or content encryption key using a public key of the wireless recipient;

signing encrypted content or content encryption key using a private key of the wireless sender; and

sending the protected content or content encryption key together with a device certificate of the wireless sender to the wireless recipient.

13. A wireless network according to claim 8, **characterized in that** the peer-to-peer forwarding/recipient of DRM protected content module of a wireless recipient verifies forwarded protected content from a wireless sender by:

verifying a device certificate of the wireless sender; and

applying a private key of the wireless recipient in order for the wireless recipient to consume the protected content.

14. A wireless network according to claim 8, **characterized in that** the protected content is digital rights management protected content.

15. A wireless terminal for operating in a wireless network having another wireless terminal and a network infrastructure for forwarding peer-to-peer content from the wireless terminal to the other wireless terminal, **characterized in that** each wireless terminal comprises a peer-to-peer forwarding/reception of DRM protected content module for either encrypting, consuming, or a combination thereof, protected content without content personalization assistance from the network infrastructure.

16. A wireless terminal according to claim 1, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender sends an initial message having an international mobile equipment identity, a sender name or mobile station international integrated subscriber digital network number to a wireless recipient.

17. A wireless terminal according to claim 15, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender personalizes the protected content for a wireless recipient.

18. A wireless terminal according to claim 17, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender personalizes the content for a wireless recipient by:

encrypting the content or content encryption key using a public key of the wireless recipient;

signing encrypted content or content encryption key using a private key of the wireless sender; and

sending the protected content or content encryption key together with a device certificate of the wireless sender to the wireless recipient.

19. A wireless terminal according to claim 15, **characterized in that** the peer-to-peer forwarding/reception of DRM protected content module of a wireless sender sends a device certificate having a public key to a wireless sender.

20. A wireless terminal according to claim 15, **characterized in that** the peer-to-peer forwarding/recipient of DRM protected content module of a wireless recipient verifies forwarded protected content from a wireless sender by:

verifying a device certificate of the wireless sender; and

applying a private key of the wireless recipient in order for the wireless recipient to consume the protected content.

21. A wireless terminal according to claim 15, **characterized in that** the protected content is digital rights management protected content.

22. A method for forwarding a protected content or content encryption key from a first terminal to a second terminal, comprising the steps of:

sending an initial message from a first terminal to a second terminal;

sending a digital rights management device certificate containing a public digital rights management key from the second terminal to the first terminal;

verifying the public digital rights management key by the first terminal;

personalizing digital rights management content or content encryption key by encryption using a public key of the second terminal;

signing encrypted digital rights management content or content encryption key using a private digital rights management key of the first terminal;

sending encrypted and signed digital rights management content or content encryption key together with a digital rights management device certificate of the first terminal from the first terminal to the second terminal;

verifying the digital rights management device certificate of the first terminal by the second terminal; and

applying a private digital rights management key of the second terminal, if the private digital rights management key of the first terminal is verified, in

order for the second terminal to consume the protected content.

23. A method according to claim 22, **characterized in that** the initial message includes a sender name, an international mobile equipment identity, a mobile station integrated service digital network number, or a combination thereof.

24. A method according to claim 23, **characterized in that** the method further comprises confirming receipt of the encrypted and signed digital rights management content or content encryption key from the second terminal to the first terminal.

25. A method according to claim 24, **characterized in that** the method further comprises sending an error message if verification of the encrypted and signed digital rights management content or content encryption key fails.

26. A method according to claim 22, **characterized in that** the sender sends an initial message having a device certificate to the wireless recipient.

27. A method according to claim 1, **characterized in that** the initial message includes a device certificate to the wireless recipient.